IA-00083

AFCEA TechNet '98
Fort Monmouth

Vulnerabilities and Threats
&
US Government Response

New Jersey

September 1998

•

Mike McConnell

Vice President, Booz-Allen & Hamilton

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 00091998	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Vulnerabilities and Threats & US Government Response	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Booz-Allen & Hamilton	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 17	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	9/25/87	Briefing

4. TITLE AND SUBTITLE
Vulnerabilities and Threats & US Government Response

5. FUNDING NUMBERS

6. AUTHOR(S)
Mike McConnell

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis
Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

This AFCEA briefing outlines information vulnerabilities and threats and the US Government response. The briefing discusses the trends in the information age, data protection over time, the evolving defense environment, threat awareness over the past, present and future, and PDD-63.

14. SUBJECT TERMS
Vulnerabilities, data protection

15. NUMBER OF PAGES

16. PRICE CODE

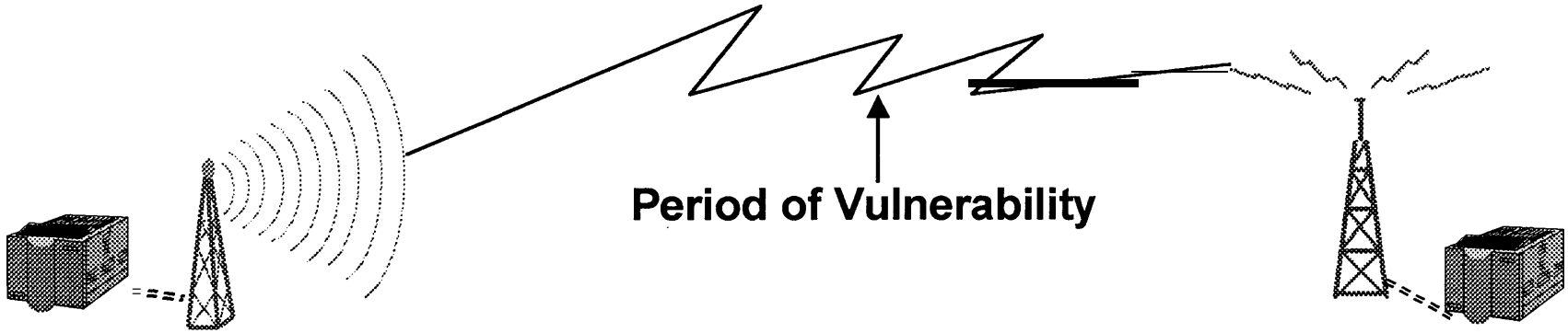
17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

Information Age Trends

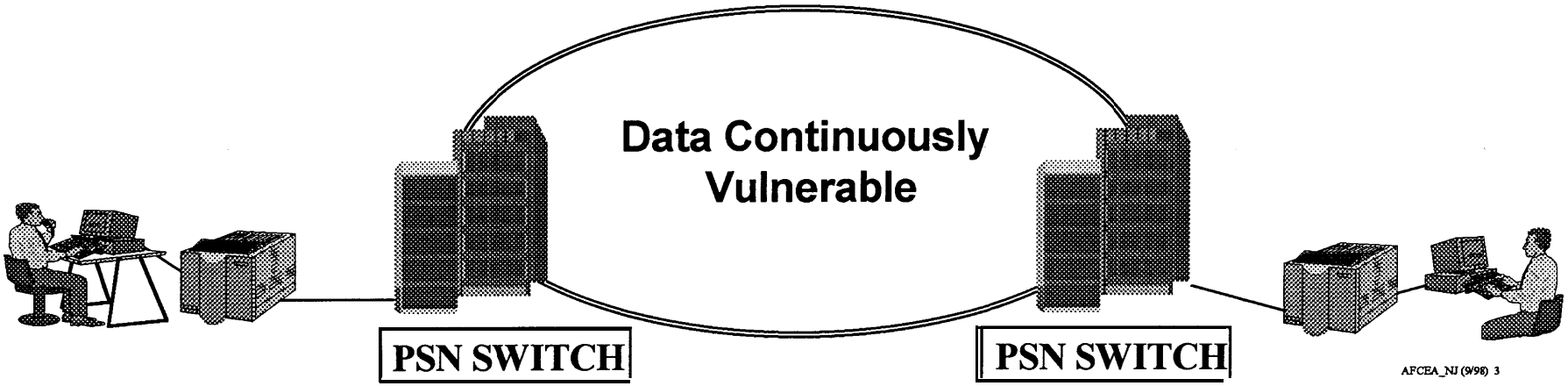
- INFORMATION has become the Primary Capital (Human Intelligence & Intellectual Capital)
- Instant Global Communications & Networking have Profound Consequences
- Public & Private Institutions and markets will be transformed
- National Boundaries are increasingly irrelevant
- Traditional Power & Perquisites of Sovereignty are Disappearing (In govt and private organizations)
- Vulnerability of Networked Information has increased

Data Protection Yesterday & Today

Data in Motion



Data in Motion *AND* at Rest



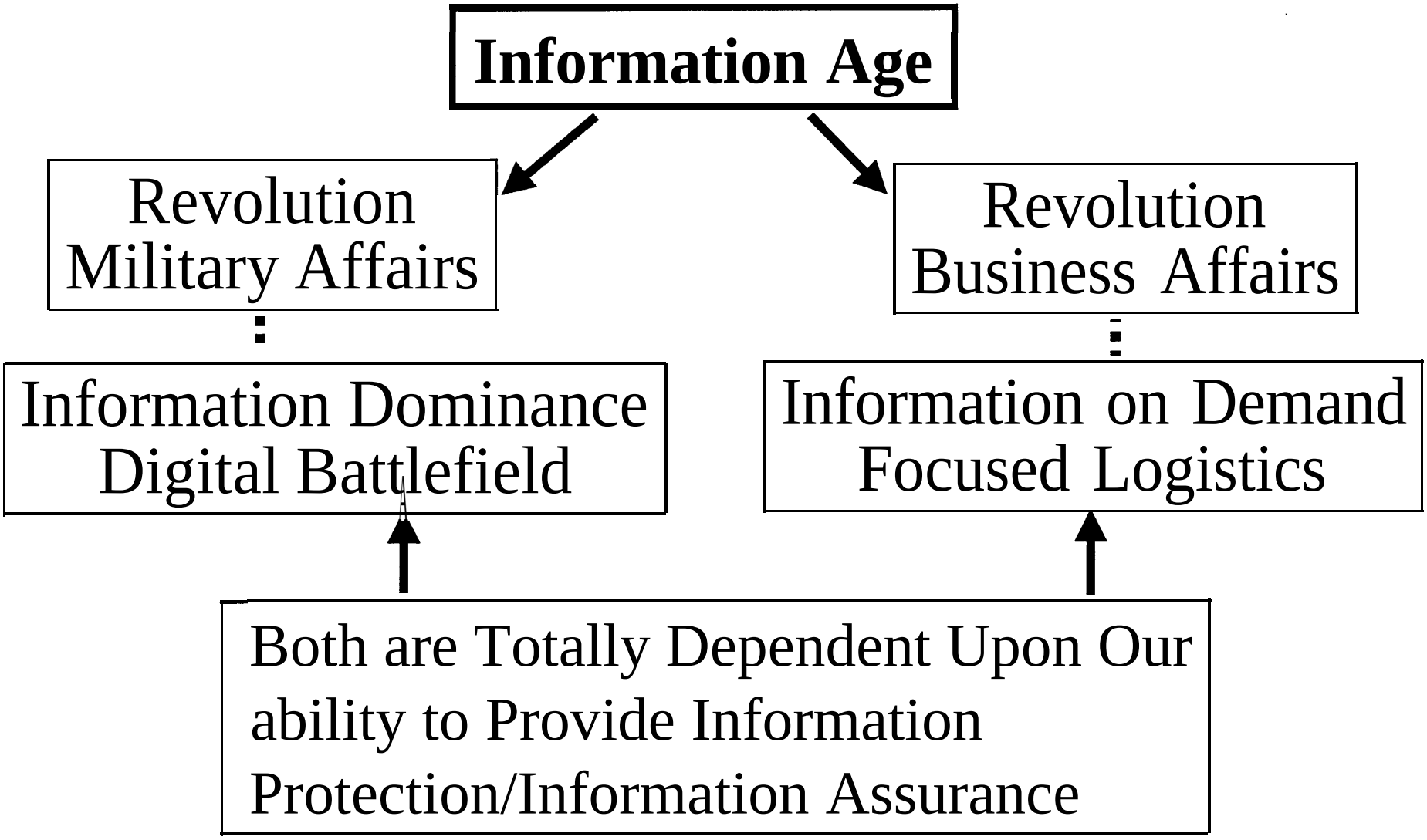
How Vulnerable Are We?

- **Massive Networking makes the US. the *World's Most Vulnerable Target* for Information Attack**
  - **Exploitation (Passive)**
  - **Disruption of Network Infrastructure (Theft-Destruction)**

- **U.S. has *Orders of Magnitude More To Lose* than other nations**

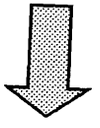
- **Reliance on Unprotected Networks carries *Risk of Military Failure, Catastrophic Economic Loss, Damage to Critical Infrastructures***

Evolving Defense Environment

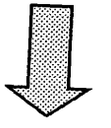


Risk Equation

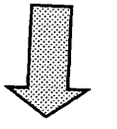
Vulnerabilities x **Threats** = **Risks**



Known



Less Known

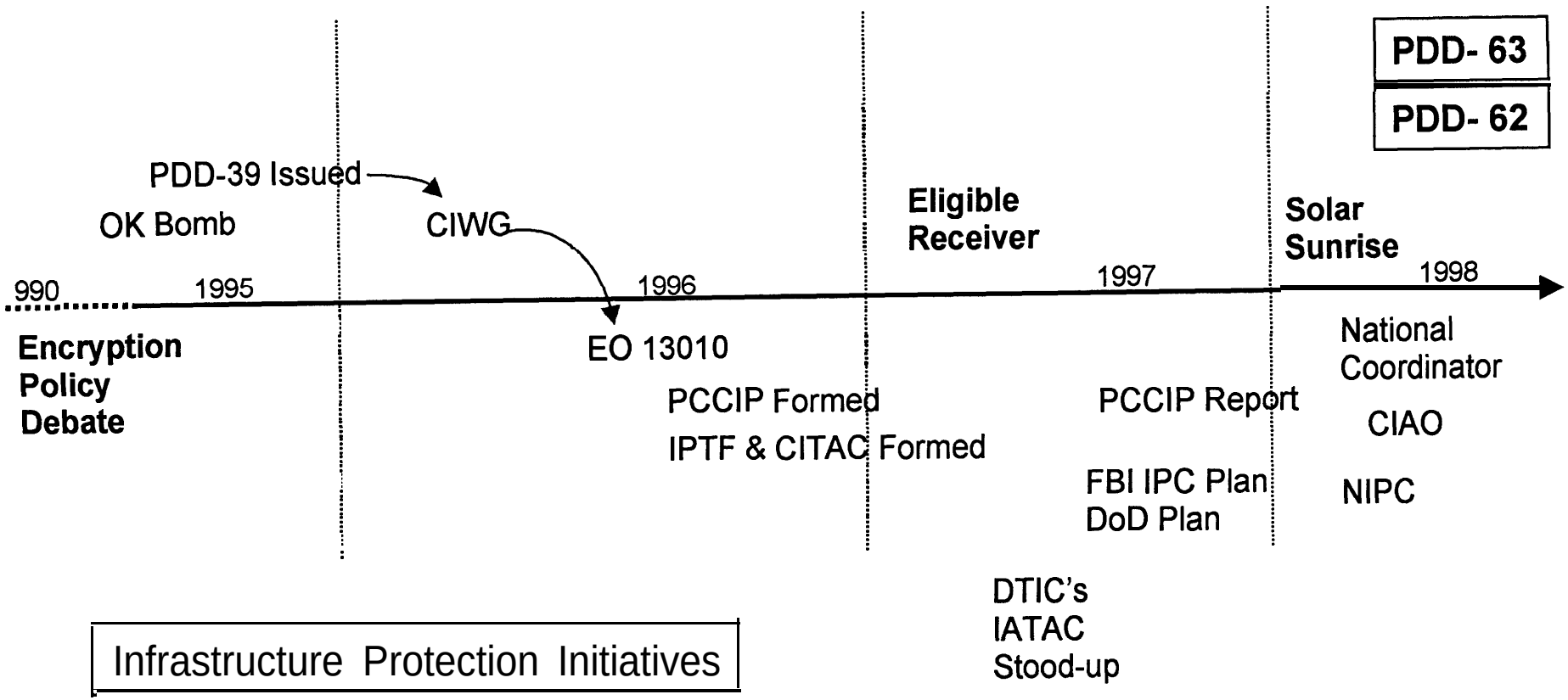


Least Understood

Threat Awareness Past/Present/Future

- Govt/Media Reports of Vulnerabilities 1993-96
- PDD-35, PDD-39 (Intelligence Priorities/Counter-Terrorism)
- Executive Order (EO) 13010 (PCCIP)
- Economic Espionage Act 1996
- Defense Science Board (DSB) IW-D Report - Nov 96
- Executive Order (EO) 13026 - Nov 96 (Encryption Policy)
- Senate Secrecy Commission - Mar 97
- Presidential Commission (PCCIP) Recommendations Oct 97
- PDD-63 (Critical Infrastructure Assurance) - May 98
- National Infrastructure Assurance Plan - May 2000

Infrastructure Assurance Timeline …

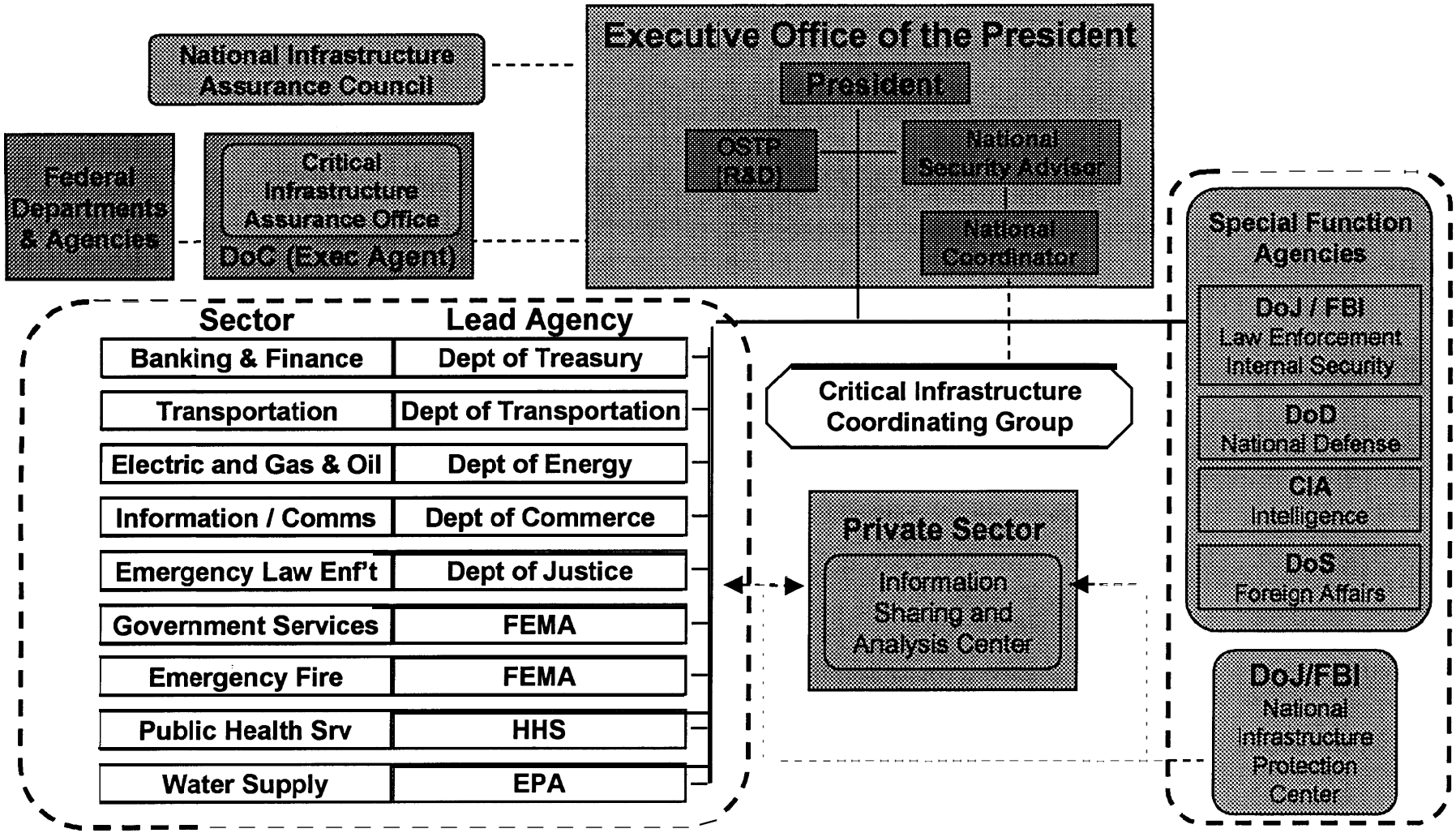


PDD 63
Vulnerability & President's Intent

- President's Recognition of "Growing Potential Vulnerability"
  - Critical Infrastructures linked and interdependent
  - U.S. heavily reliant upon networked systems
  - Cyber threat is real

- President's Intent: "U.S. will take all necessary measures..."
  - To eliminate any significant vulnerability to U.S. physical or cyber attacks on our critical infrastructures

PDD-63 Organization



PDD 63
Public-Private Partnership

- Since critical infrastructures are mix of public-private stakeholders, elimination of potential vulnerability requires closely coordinated effort between public and private sector
  - To succeed, must be "genuine, mutual and cooperative"
  - Avoid, where feasible, increased government regulation and unfunded mandates
  - Appoint Sector Liaison to work with private industry Sector Coordinator

PDD-63
Every Department / Agency ...

- **Shall be responsible for protecting its own critical infrastructures**
- **CIO will be responsible for Information Assurance**
- **Shall appoint a Critical Infrastructure Assurance Officer (CIAO) responsible for protection of all the other aspects o that department's critical infrastructure**
- **Develop a plan for protecting its own critical infrastructure, no later than 180 days from the PDD**

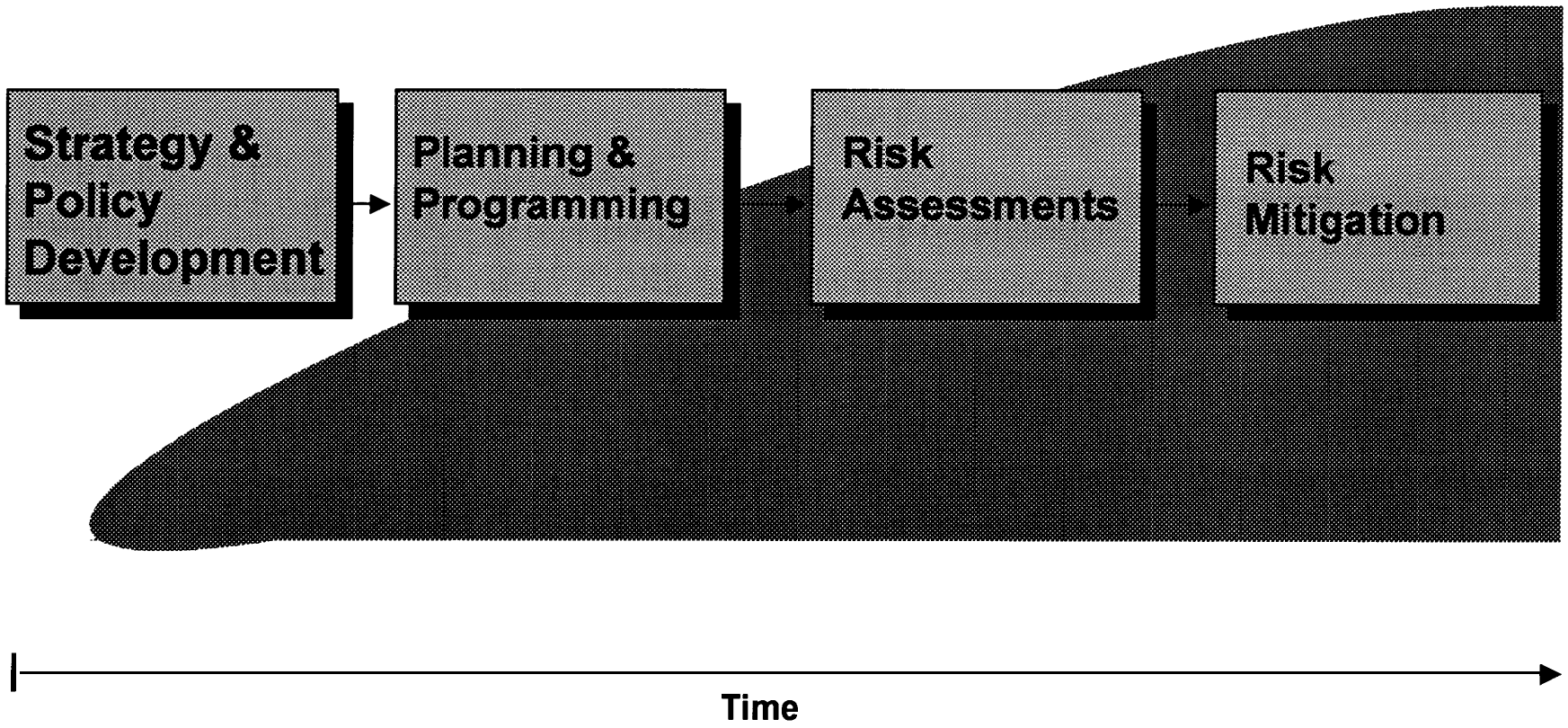
PDD 63
National Infrastructure Protection

- **By 2003 achieve ability to protect nation's critical infrastructures from intentional acts that would diminish the ability of:**
  - **The Fed govt to perform essential national security missions and ensure the public health and safety**
  - **State & Local governments to maintain order and to deliver minimum essential public services**
  - **The Private Sector to ensure the orderly functioning of the economy & the delivery of essential telecomm, energy, financial, and transportation services**

PDD-63
Task Areas

- Vulnerability Analyses
- Remedial Plan
- Warning
- Response
- Reconstitution
- Education & Awareness
- Research & Development
- Intelligence
- International Cooperation
- Legislative & Budgetary Requirements

PDD-63 Requirements



“At the end of the day,...”

- **Vulnerabilities**
  - **Real but not Widely Recognized**
  - **Governments Just Beginning to Focus**
  - **Industry is Not Focused on this issue**
- **Threat**
  - **Real, but Difficult to Quantify**
  - **Government is Changing Focus from Traditional Threat to Information Age Threat**
  - **Industry Barely in the Acceptance Stage**
- **Risks Exist But**
  - **Understood by Only a Small number of People**
  - **Government - Still Trying to Define**
  - **Industry - Nowhere near Consensus**